AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of South Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple iPhone 6 Plus Cellular Telephone IMEI # is 355722070579719; Model: A1634

Case No. 2:18 cr 194

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the _____ District of South Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1343	Wire Fraud

The application is based on these facts:

See Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Chris Goode
Applicant's signature

Christopher Goode, TFO, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: Jan 31, 2018

Judge's signature

City and state: Charleston, SC

The Honorable Bristow Marchant, Magistrate Judge
Printed name and title

CG

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA

IN THE MATTER OF THE SEARCH OF **Apple iPhone 6 Plus Cellular Telephone IMEI # is 355722070579719; Model: A1634** CURRENTLY LOCATED AT **Mount Pleasant Police Department at 100 Ann Edwards Ln Mount Pleasant, SC 29464**	Case No. 2:18cr194

AFFIDAVIT IN SUPPORT OF AN APPLICATION

UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Chris Goode, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the following property: an electronic device, which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am a Task Force Officer ("TFO") with the United States Drug Enforcement Administration ("DEA") and have been assigned to DEA since January of 2017. I have been a sworn law enforcement officer for the Mount Pleasant Police Department ("MPPD") since August of 2011. I was first assigned to the patrol division and patrolled the streets of Mount Pleasant, SC in a uniform and a marked police car. In September of 2013, I was assigned as a detective in the Mount Pleasant Police Department Narcotics Unit. My duties and responsibilities focused on drug investigations and drug traffickers in the jurisdiction of the Town of Mount Pleasant, SC.
3. During my tenure as a police officer and narcotics detective, I have received over 300 hours of specialized narcotics training through various programs, which are recognized by the South Carolina Criminal Justice Academy, and through various courses with the High Intensity Drug Trafficking Area ("HIDTA") program. I have also received advanced training and received certification in the use of Cellebrite mobile forensics. In January of 2017, I was assigned to the Drug Enforcement Administration Task Force, and my duties and responsibilities shifted to investigating drug

CG

traffickers operating inside the borders of the United States. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7) and am empowered by federal law to investigate and make arrests for offenses enumerated in Section 2518 of Title 18 of the United States Code.

4. As a TFO, I have been trained in various aspects of law enforcement, particularly the investigation of narcotics offenses and drug trafficking organizations. During my experience as a police officer/narcotics detective with MPPD and as a TFO with the DEA, I have participated in numerous drug investigations and prosecutions and have testified as an expert witness on narcotics investigations for a state court case in 2016. Additionally, I have arrested, or participated in the arrest of, numerous individuals for their violations of narcotics laws governed by federal and/or state statutes. In connection with those investigations, I have conducted multiple undercover operations, controlled drug transactions with the use of cooperating sources, surveillance operations (mobile and stationary), executed search warrants, informant/suspect debriefs and interviews, electronic surveillance, pen registers/trap and trace devices, and secured relevant information using numerous other investigative techniques, including the use of Cellebrite mobile phone forensics extractions. I have personally participated in two court-authorized Title III investigations.
5. Based upon my training and experience in conducting drug investigations, interviewing defendants/witnesses/informants, and executing Cellebrite mobile phone extractions of participants in drug distribution/trafficking activity I am familiar with the ways in which drug traffickers conduct their business. Furthermore, I am familiar with the various means and methods by which drug traffickers import and distribute drugs, use cellular telephones, text messages, and third party applications on their phones to facilitate drug activity, and use numerical codes and code words to conduct their drug transactions. I have been assisted in this investigation by DEA Financial Investigator Steven Migioia (retired DEA Special Agent) who has received extensive training in both narcotics and financial investigations. Investigator Migioia has completed basic and advanced asset forfeiture/financial investigation training at the DEA academy. He has also completed basic and advanced money laundering techniques, as provided by the Asset Forfeiture Money Laundering Section of the Department of Justice.
6. I am currently assigned to the Charleston, South Carolina DEA Task Force. The Task Force consists of federally deputized officers and special agents from the DEA, Mount Pleasant Police Department, Charleston County Sheriff's Office, North Charleston Police Department, South Carolina Highway

CG

Patrol, Summerville Police Department, Charleston Police Department, Dorchester County Sheriff's Office, Hampton County Sheriff's Office, and Berkley County Sheriff's Office. I am acting as the co-case agent and am responsible for coordinating and overseeing all aspects of this investigation. As a co-case agent, I am thoroughly familiar with the information contained in this affidavit, either through personal investigation or through discussions I have had with other agents/officers who have conducted interviews or who have themselves obtained information, which they in turn have reported to me.

7. I have personally participated in this investigation and am aware of the facts contained herein based upon my own investigation as well as information provided to me by other law enforcement officers. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a complaint, I have not set forth all of my knowledge about this matter.

IDENTIFICATION OF DEVICE TO BE EXAMINED

8. The property to be searched is a black and gray Apple iPhone 6 Plus cellular telephone, IMEI # 355722070579719; model: A1634), hereinafter "Target Telephone 1." The Device is currently secured in evidence at the Mount Pleasant Police Department at 100 Ann Edwards Ln Mount Pleasant, SC 29464.
9. The applied for warrant would authorize the forensic examination of Target Telephone 1 for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

10. On August 11, 2017, the Mount Pleasant Police Department responded to a drug overdose which resulted in death at Tyler SCHER's (hereinafter "SCHER") residence, 1758 Parc Vue in the Montclair Subdivision in Mount Pleasant, SC. A lawful search warrant was conducted at the residence and detectives located various items of drug paraphernalia and also seized a quantity of white powdery substance, which was later confirmed though the South Carolina Law Enforcement Division Forensic Services Laboratory to be fentanyl. Detectives also seized the cell phone SCHER had at the time. SCHER was arrested for Possession with Intent to Distribute Heroin. SCHER was later released on bond. The August 11, 2017 cell phone was eventually searched pursuant to a proffer agreement executed September 25, 2017. The August 11, 2017 cell phone is not the subject of this affidavit.

CG

11. The Mount Pleasant Police Department Criminal Investigations Unit received a complainant/report from a victim, Mr. Peter Tyson, regarding financial crimes involving SCHER. SCHER advertised his apartment, 1758 Parc Vue, on the website "Airbnb" in efforts to rent his room for a short period of time for money. On September 10, 2017, the victim, Mr. Peter Tyson, contacted SCHER and expressed his interest in renting the room at SCHER's apartment. Mr. Tyson sent SCHER a personal check (Check # 549; Dated: 09/13/2017) from Meredith Villages Savings Bank (Routing Number: 211772936; Account Number ending in XXXX6698) in the amount of $975.00 to pay for the room in advance.

12. On September 13, 2017, SCHER contacted the victim, Mr. Tyson, and informed him that the room was no longer available for rent. SCHER told Mr. Tyson that since the room was not available, he (SCHER) would destroy the check that Mr. Tyson sent him. However, the check Mr. Tyson sent to SCHER was never destroyed but instead it was mobile deposited into SCHER's TD bank account on October 25, 2017 at 12:40:17 PM. The "mobile deposit" indicates that SCHER used an application on a mobile device that allowed SCHER to take a photo of the victim's check to deposit the funds into SCHER's account. It is common for mobile device application to be used from a cell phone for customer convenience.

13. On December 14, 2017, Mr. Tyson and a member of risk management for Meredith Village Savings Bank in New Hampshire, Mr. Mike Nolan, notified Sgt. Salata of multiple unauthorized withdrawals from Mr. Tyson's account. Mr. Nolan provided Mr. Tyson's account bank records showing the unauthorized transactions were conducted by SCHER. Mr. Nolan also provided a copy of the victim's check image which showed that SCHER "mobile deposited" the check into his (SCHER's) bank account. The financial records showed that between November 21, 2017 and December 4, 2017, approximately seven (7) online transactions were conducted from the victim's bank account to a Chase Credit Card and Capital One Credit Card account in Tyler SCHER's name. The victim's financial documents (provided by the victim and Mr. Nolan) show that SCHER, without the victim's permission, unlawfully transferred approximately $16,007.70 from the victims account to make payments towards SCHER's personal credit cards.

14. On January 23, 2018, Sgt. Salata obtained a state arrest warrant for Tyler SCHER for Financial Identity Theft. Shortly after the arrest warrant was obtained, at approximately 1445 hours, TFO Goode and MPPD PFC. Harper located and arrested Tyler SCHER at his residence, 1758 Parc Vue, in Mount Pleasant, SC. During the arrest, SCHER asked law enforcement to get his phone and

CG

stated it was on the living room coffee table. Law enforcement found the phone and asked SCHER if that was his phone he had referred to. SCHER said yes. The officers then took SCHER outside. SCHER stated he wanted to get a number out of his phone. Law enforcement held the phone while SCHER used the phone to retrieve the number. Law enforcement placed the phone into evidence at MPPD. Law enforcement observed SCHER type his passcode into the phone when he retrieved the contact information.

15. That based on the financial records, SCHER utilized the "mobile deposit" application on his cellular device to deposit the victim's $975.00 check into SCHER's own account. SCHER was able to obtain the victim's bank account and routing numbers from the bottom of the victim's check. SCHER then used the victim's personal account information to conduct online (web/internet based) payments from the victim's account to SCHER's personal accounts. That there is probable cause that SCHER utilized his cellular phone to aid in the unlawful electronic transfer/payment of funds (EFT) from the victim's bank account to SCHER's own personal credit card accounts. The incriminating nature of the cell phone was immediately apparent at the time it was seized, and the evidence contained on the device could have been destroyed if officers did not seize it at the time.

16. On January 24, 2018, Financial Investigator Steven Migioia received information from a Capitol One Investigator confirming that Tyler SCHER had three Capitol One credit card accounts. Furthermore, the Capitol One investigator confirmed that on approximately November 20, 2017, an EFT was conducted from Mr. Tyson's Meredith Villages Savings Bank (Routing Number: 211772936; Account Number Ending In XXXX6698) to Tyler SCHER's Capitol One credit card ending in XXXX5062. This fraudulent transaction also resulted in a loss to Capitol One.

17. The victim's established residence and the victim's financial institution, Meredith Village Savings Bank, are both located in the state of New Hampshire. The suspect, Tyler SCHER, who at the time of the wire fraud resided at 1758 Parc Vue Ave. Mount Pleasant, SC. Records furnished by Capital One, documented that SCHER used a service provider with the assigned IP 73.180.116.246. This IP address is associated with Comcast. Comcast is a cable and internet provider with nationwide service. The EFT conducted on November 20, 2017, by SCHER utilized IP address 73.180.116.246 from the residence 1758 Parc Vue Ave. Mount Pleasant, SC which establishes an interstate nexus in connection with violations of Title 18, United States Code, Section 1343.

CG

TECHNICAL TERMS

18. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications, I know that the device, an Apple iPhone 6, has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device(s), and PDA as well as providing connectivity to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices and the criminal nature for what they were using the device.

19. Furthermore, I know that Apple iPhone devices can auto wipe/erase all data if a person attempts to enter an incorrect password a number of times. I know that Apple iPhone devices have capabilities that allow owners or authorized users to remote wipe (erase all data) the data on the cellular device even if the owner/user is not in possession of the device. In an effort to preserve the possible evidence/data stored on the cellular device, the device was seized and secured into evidence for safekeeping until a search warrant could be issued.

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

    a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device(s) used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device(s).

CG

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device(s) designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device(s) uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation device(s) can give a user driving or walking directions to another location. These device(s) can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A Personal Digital Assistant, or PDA, is a handheld electronic device(s) used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication device(s) and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable

CG

storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device(s).

f. An Apple iPhone can function as is a mobile computer and is primarily operated by a touch screen. An Apple iPhone can work as a wireless communication device and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. A device typically contains programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic device(s) that communicate with each other. Due to the structure of the Internet, connections between device(s) on the Internet often cross state and international borders, even when the device(s) communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

CG

22. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device(s) was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device(s) works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic device(s) were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device(s) was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim's account over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence

CG

of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

23. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e) (2) (B), the warrant I am applying for would permit the examination of the device(s) consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device(s) to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution*. Because this warrant seeks only permission to examine a device(s) already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the device(s) described in Attachment A to seek the items described in Attachment B.

26. This applied-for warrant would authorize the forensic examination of the device(s) for the purpose of identifying electronically stored data particularly described in Attachment B, see also Attachment C.

Respectfully submitted,

Christopher J. Goode
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me
On 31st day of January, 2018.

THE HONORABLE BRISTOW MARCHANT
UNITED STATES MAGISTRATE JUDGE

CG